Future Computing Environment and Issues of Security

David B. Nelson, Ph.D., CISSP

Director

National Coordination Office for

Information Technology Research and Development

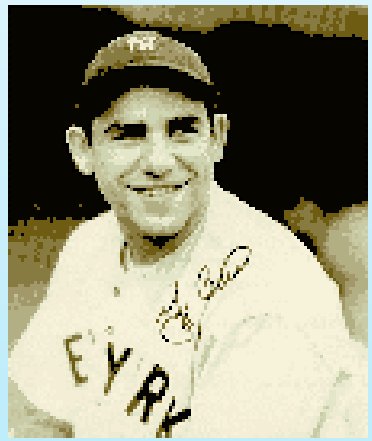
November 5, 2003

George Mason University

Looking Ahead Helps Us Prepare, However ...

“Predicting is tricky, especially about the future”

–Yogi Berra



Likely Characteristics of Future Computing Environment

- **Critical to the enterprise**
  - Agent for most business
  - More robust and self-regulating (autonomic computing)
- **Widely distributed**
  - "The network is the computer" - Scott McNealy
  - Use of middleware: Grid services, Web services, collaboration tools
  - Computing on demand using remote resources
- **Ubiquitous**
  - Always available by wireless and wired connections
  - Portable identity and workspace
  - Human-centric with improved collaboration, communication, and resource discovery tools
- **Heterogeneous**
  - Many different kinds of devices with different power and characteristics
  - Alternative technologies for organization/presentation of data

Likely Characteristics of Future Computing Environment

- **Extended beyond organizational boundaries**
  - Virtual organizations
  - Membership and trust issues
- **Dynamic**
  - Discovery and use of resources
  - Management and configuration issues
- **Mediated by middleware**
- **Challenging to maintain security**
  - Hard to determine what is inside vs. outside
  - Hard to determine appropriate usage/users for identity, authentication, authorization
  - Web Services will mean port 80 is used for "everything"
  - Increasing demands for privacy and anonymity
  - Need for role-based security
- **If we are very lucky, perhaps re-designed to be more intrinsically secure**

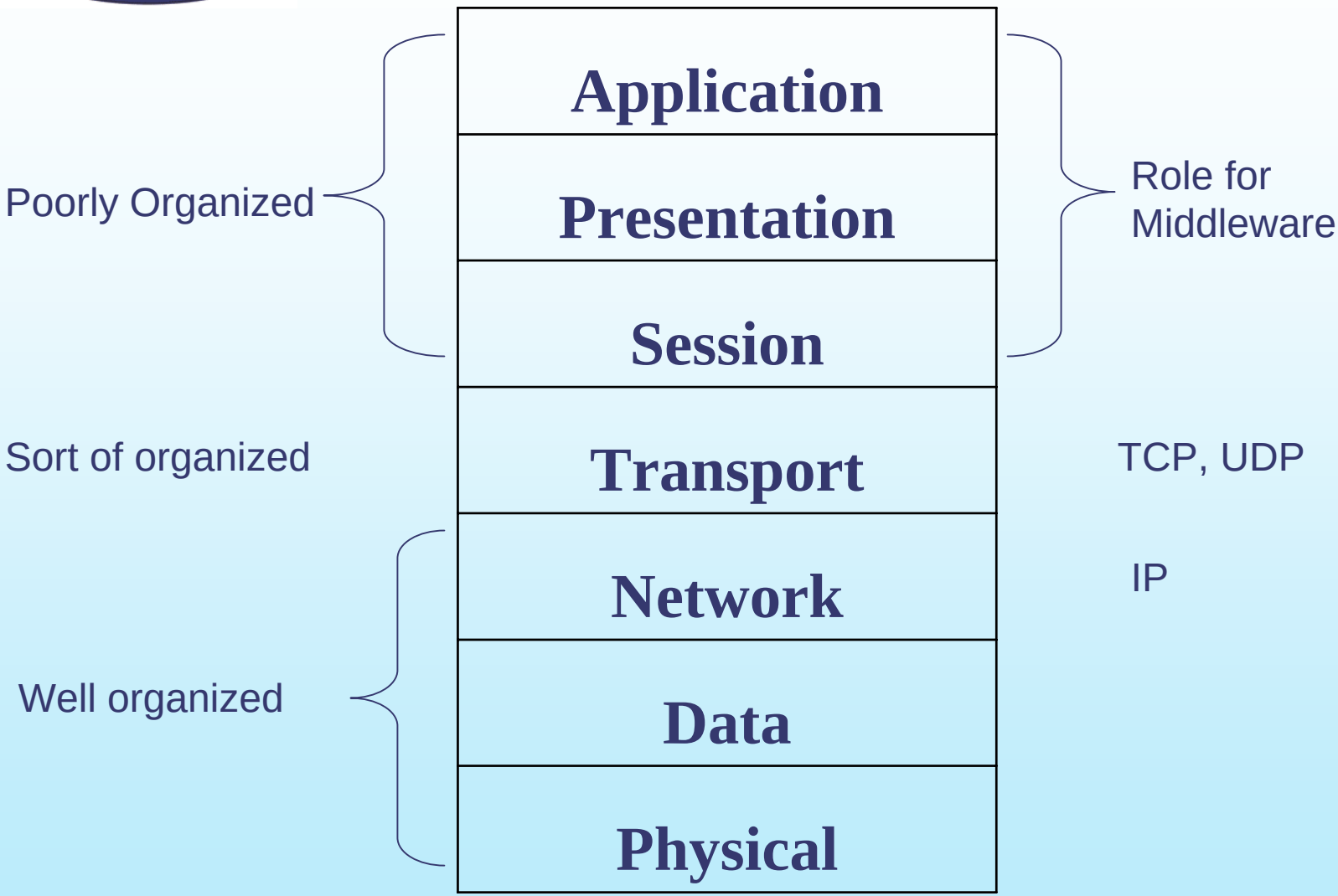
Security Concerns Are Also Evolving

- **Classic security concerns deal more with data**
  - Confidentiality (data only available to those authorized)
  - Availability (you can get it when you want it)
  - Integrity (data hasn't been changed)
- **Additional concerns deal more with people and transactions**
  - Trust (Who you are and what you are authorized to do)
  - Non-repudiation (You can't deny doing something you did)
  - Auditability (I can check what you did to the data)
  - Reliability (The system does what I want when I want it to)
  - Privacy (Within certain limits no one should know who I am or what I do)
  - Some of these were "solved" in stand-alone mainframe environment; much harder in networked environment

Security Challenges of Future Computing Environment

- How to accommodate vision of distributed large-scale collaborations, access to resources, eCommerce, without compromising security?
- How to accommodate dynamic computing environment within current framework of security risk management?
- How to evolve security practices and technologies to keep up with future computing environment?
- How to build security into architecture of future environment, including ability to withstand, identify, and respond to attacks?
- How to say “yes” rather than “no” to users and developers without compromising security?

Middleware Is Software That Helps Organize ISO Network Layers 5-7



ISO 7-layer Network Model

Grid Computing: Example of Distributed Computing Enabled by Middleware

- **Goal: Enable a geographically distributed community [of thousands] to perform sophisticated, computationally intensive analyses on Petabytes (10^{15} bytes) of data**
- **Organizations coordinating Grid tools and security**
  - Global Grid Forum www.ggf.org
  - Globus Project www.globus.org
- **Standards: Open Grid Services Architecture, Open Grid Services Infrastructure (uses Web services)**
- **Globus Toolkit™ centers around four key protocols**
  - *Security*: Grid Security Infrastructure (PKI, X.509 certificates, SSL, extensions for single sign-on and delegation)
  - *Resource Management*: Grid Resource Allocation Management
  - *Information Services*: Grid Resource Information Protocol
  - *Data Transfer*: Grid File Transfer Protocol (GridFTP)

Examples of Data Grid Projects

- **European Data Grid (EU)**
  - DG technologies & deployment in EU
- **GriPhyN (NSF)**
  - High Energy Physics, Investigation of "Virtual Data" concept
- **Particle Physics Data Grid (DOE Science)**
  - DG applications for HENP
- **Earth System Grid (DOE Science)**
  - DG technologies, climate applications
- **Information Power Grid (NASA)**
  - DG applications

Particle Physics Data Grid

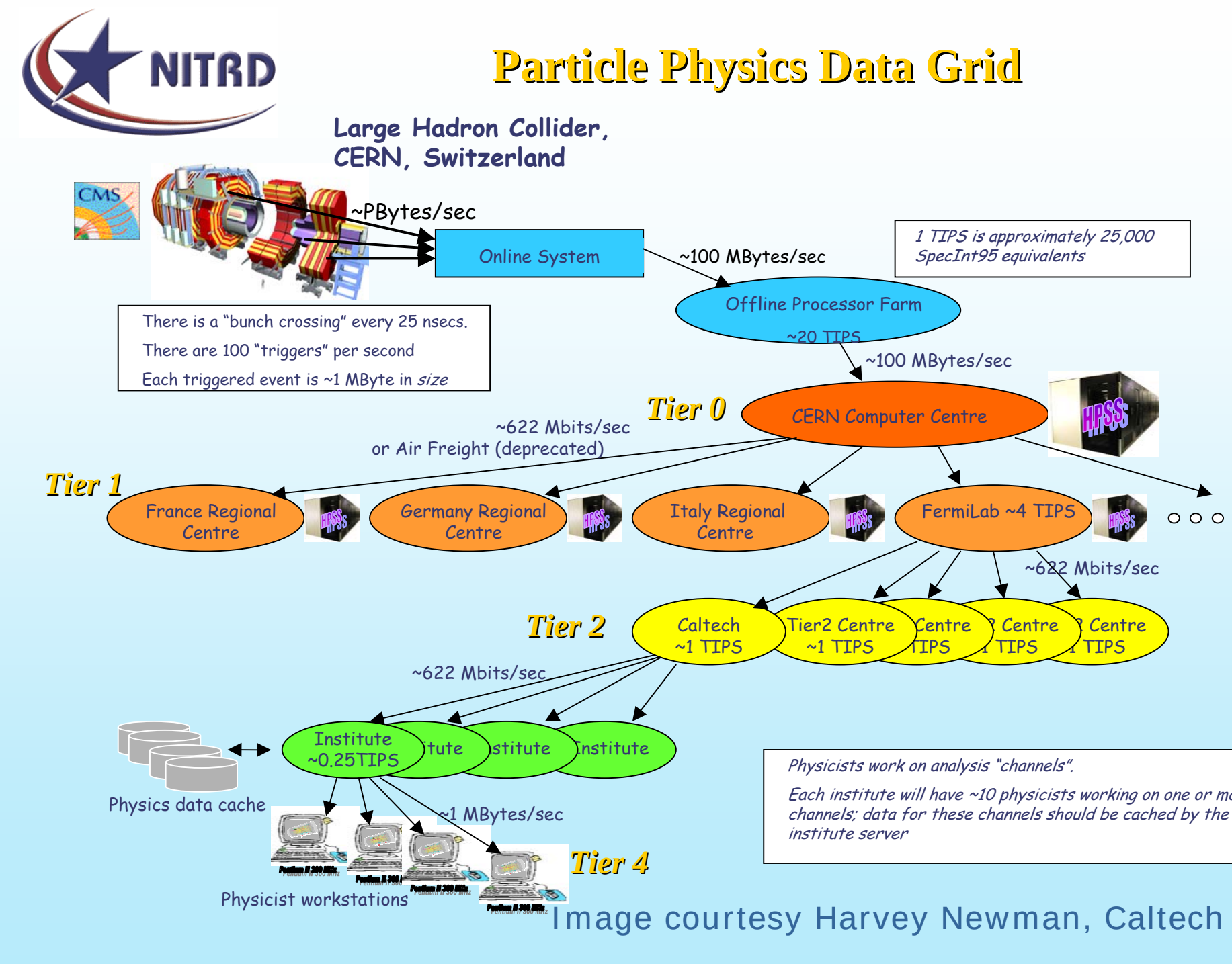
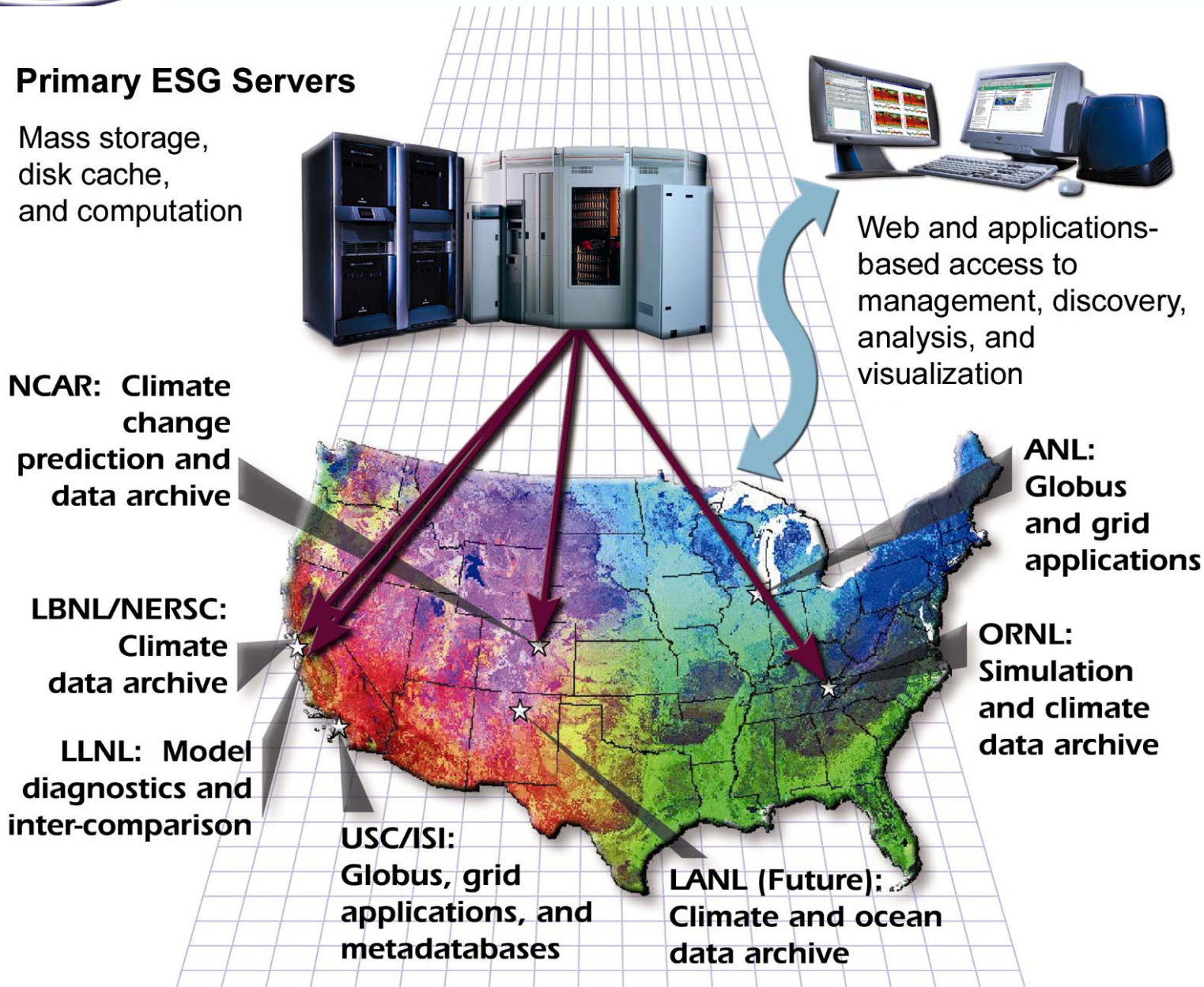


Image courtesy Harvey Newman, Caltech

Earth System Grid



Security Implications of Grid Computing

- **Need to allow access to trusted sources, but how do you determine trust in a dynamic community of thousands (or more) in different organizations?**
- **Need to allow Web services on port 80 (HTTP) or port 443 (SSL, HTTPS) through the firewall**
  - Application level firewalls
- **Companies such as IBM, HP, and Microsoft offer commercial grid software and services, but typically only for Intragrids (inside organizations) where security can be managed coherently**
- **The more interesting security issue is the virtual organization or Intergrid**
  - Unsolved problem, because current solutions create Federations of Enterprises based on pair-wise trust agreements; these don't scale

Security Implications of Grid Computing

- **Today Globus Toolkit uses Public Key Infrastructure for both authentication and authorization**
- **Some experts advocate using PKI only for authentication (based on a certificate authority)**
- **Use directory services for authorization (probably LDAP) with communication through Security Assertion Markup Language (SAML)**
  - Shibboleth is a reference implementation http://shibboleth.internet2.edu
- **SAML is a web-based language (over HTTP) that allows three kinds of messages:**
  - Attribute assertions
  - Authentication assertions
  - Authorization assertions
- **For some transactions we need to add privacy**
  - How to anonymize identity, attributes, actions, and personal data?
  - Being researched as part of the DARPA Total Information Awareness project

Why should we care about privacy?

- **History has shown that available information can be abused to persecute individuals with differing beliefs**
  - Nazi Germany
  - Stalinist Russia
  - Maoist China
  - Iraq under Hussein
- **Even in the US**
  - Exile of Nisei from coastal California in WW2
  - McCarthy anti-Communist hearings
  - CIA domestic spying (Church committee hearings of 1973)
- **Laws explicitly safeguard some information privacy**
  - Gramm-Leach-Bliley Act covers privacy of financial records
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA) covers privacy of medical records
  - European Union Directive 95/46 covers protection of personal data

Example of Middleware: Web Services

- Architecture and program interfaces that enable application-to-application communication
- Run primarily on top of http (or https) web protocols
- Allow aggregation of functions provided by heterogeneous software modules, including legacy apps
- Allow changes to underlying components without manual reprogramming
- Allow seamless extension of functions and services

Web Services are Emerging Standards for eCommerce

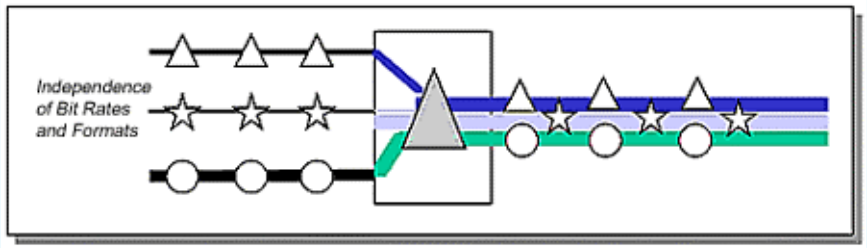
- XML (Extensible Markup Language) defines a universal way of representing any data; allows exchange of data between any applications regardless of operating system, language, hardware, user device
- SOAP (Simple Object Access Protocol) defines universal Web service requests using XML messages, making process integration simple
- WSDL (Web Services Definition Language) specifies information needed for integration among applications
- UDDI (Universal Description, Discovery, and Integration) is a Web service that allows users and applications to locate other Web services

Security in Web Services is Just Being Developed

- **HTTPS/SSL for secure point-to-point communication with known trusted parties, but**
  - no authorization, auditing, non-repudiation
  - not end-to-end, stops at HTTPS server
  - no digital signature verification through to the data base
- **WS-Security: message level security protocol**
  - persists end-to-end
  - interoperable with web services such as SOAP, SSL, Kerberos, PKI, SAML, etc.
  - http://www-106.ibm.com/developerworks/library/ws-secmap/
- **Managing trust issues is still a challenge**

Future of Network Technology*

- **Optical transmission - pushing the limits of fiber**
  - –Ultimate bandwidth of a fiber
  - –Wavelength division multiplexing
  - –Wavelength (λ) switching
  - –Fiber to the home – problems of economics (sunk cost) and technology (interconnects)



Merges *optical* traffic onto one common fiber
Allows high flexibility in expanding bandwidth
Reduces costly mux/demux function, reuses *existing* optical signals
Individual channels use original OAM&P

DWDM = Dense WDM

- **Optical switching - the chip of networking?**
  - Today it is done with mirrors
  - Need lower power optical switches
  - Would have substantial effect on computing also
- **Quality of Service vs. Over-provisioning**
  - QoS called for but hasn't emerged
  - Over-provisioning expensive but easy
  - λ switching can create circuits – a middle ground

*Thanks to George Strawn, NSF, for some of this material

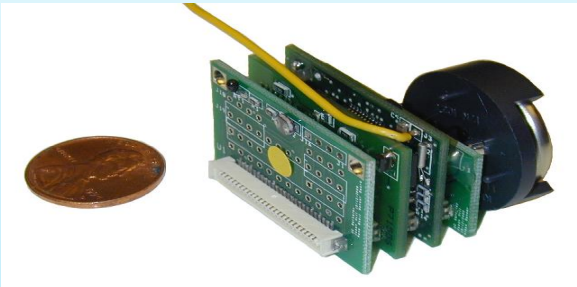
Future of Network Technology*

- **End-to-end (e2e) high performance is hard to achieve (even with network head room)**
  - 50 Mb/sec. on 1 Gb/sec. Paths
- **Applications requiring e2e high performance are slow to emerge**
  - ftp as Grid killer-ap
  - We "forget" that Internet applications requiring low performance were slow to emerge, too!
  - High Definition Video?
- **How to build firewalls running at wire speed**
- **Wireless access everywhere--ad hoc nets**
  - Self organizing
  - Cheap devices
  - Mems-based sensors
  - Energy storage limitations – fuel cells?
  - Benefit from IPv6

*Thanks to George Strawn, NSF, for some of this material

"Smart Dust"

- **UC Berkeley Project sponsored by DoD and Intel**
- **Near-Term goal: millimeter sized sensor and communication package**
  - RF, laser, modulated corner reflector
  - Temperature, humidity, pressure, light intensity, magnetic field, acceleration
- **Could be used for environmental monitoring or surveillance**
- **Experiment: air dropped swarm that spotted and tracked vehicles**
  - Magnetometer, self organizing rf network, Tiny OS



Business Models*

- **Peer-to-peer makes all clients into servers**
  - Kazaa model (major consumer of university bandwidth)
  - Groove Networks model
  - Logistical Computing and Internetworking model http://loci.cs.utk.edu/
- **Open standards and open source change the nature of competition**
- **Whither Intellectual Property?**
- **Disruptive technologies - tool of capitalist creative destruction (Where have all the mainframe makers gone?)**
- **Will networking fragment the firm by reducing transaction costs?**
  - Ronald Coates – theory of transaction costs, Nobel Prize 1991

*Thanks to George Strawn, NSF, for some of this material

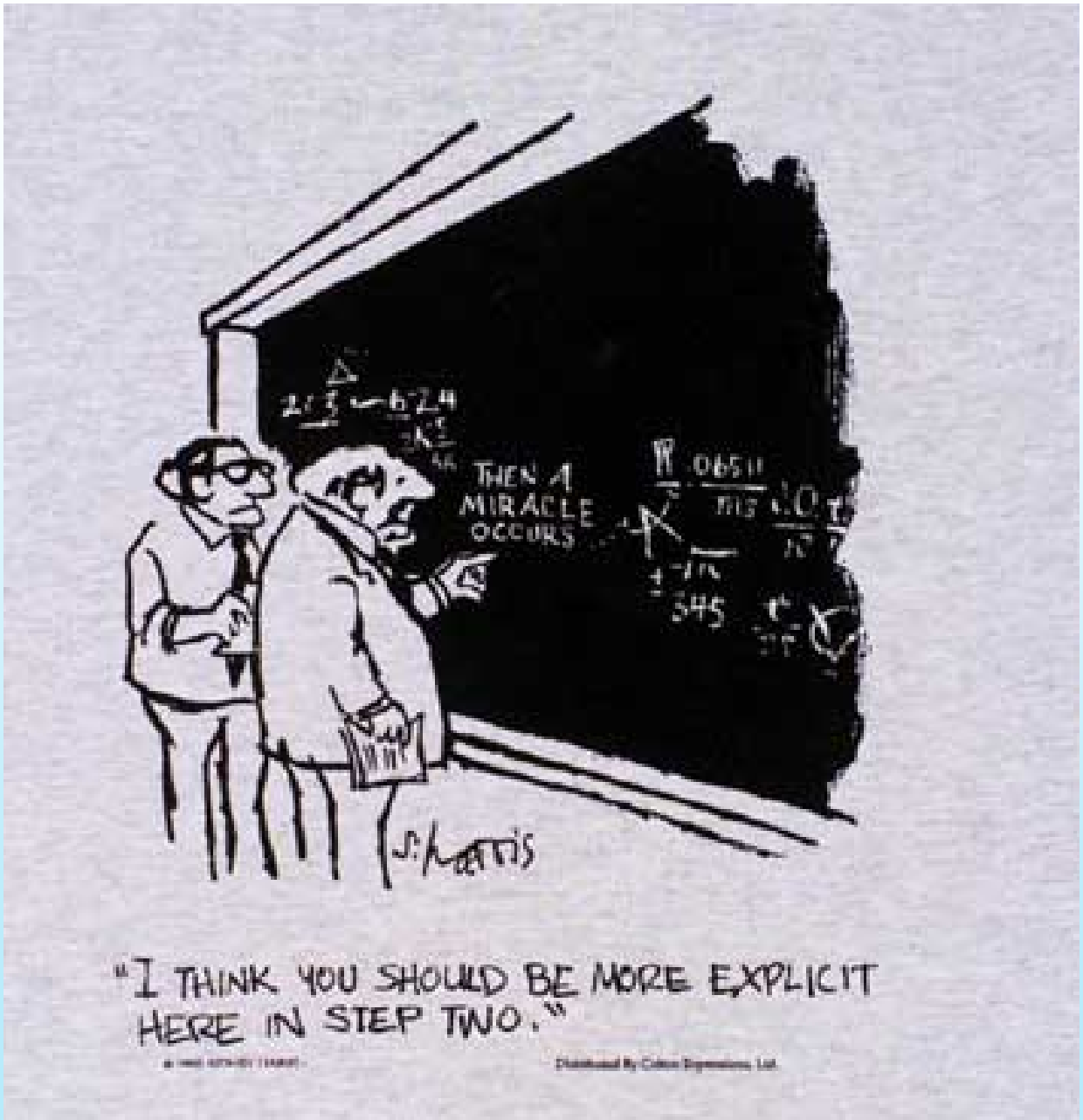
Emerging Issue of Role-Based Security

- **Role based security: Each of us assumes different roles with different security requirement. One individual may act as:**
  - Manager signing timecards or authorizing procurement
  - Researcher working on data with foreign collaborators
  - Individual buying books from Amazon.com at lunch hour
- **How to handle these different roles using common equipment (PC, network)?**
- **Alternative is separate networks and equipment for each role that requires a different levels of security or access - cumbersome and impractical**

Summary

- Future computing environment is likely to be more enterprise-critical, distributed, and dynamic than today
- Maintaining security will be challenging
- Probably new inventions will be needed (architecture, protocols, software, etc.)

Then a Miracle Occurs



For Further Information

Please contact us at:

nco@itrd.gov

Or visit us on the Web:

www.itrd.gov